JEROME C. ROTH (State Bar No. 159483)
jerome.roth@mto.com
JONATHAN H. BLAVIN (State Bar No. 230269)
jonathan.blavin@mto.com
LAURA K. Lin (State Bar No. 281542)
laura.lin@mto.com
MUNGER, TOLLES & OLSON LLP
560 Mission Street
Twenty-Seventh Floor
San Francisco, California 94105-2907
Telephone: (415) 512-4000
Facsimile: (415) 512-4077

Attorneys for LinkedIn Corporation

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

HRL

CV 14 0068

LinkedIn Corporation,

Plaintiff,

vs.

Does, 1 through 10 inclusive,

Defendants.

Case No.

Complaint For:
(1) VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. §§ 1030 ET SEQ.;
(2) VIOLATION OF CALIFORNIA PENAL CODE § 502;
(3) VIOLATION OF THE DIGITAL MILLENNIUM COPYRIGHT ACT, 17 U.S.C. §§ 1201 ET SEQ.;
(4) BREACH OF CONTRACT;
(5) TRESPASS; AND
(6) MISAPPROPRIATION

Plaintiff LinkedIn Corporation ("LinkedIn" or "Plaintiff"), by and through its attorneys, brings this Complaint against Defendants Does 1-10 (collectively, the "Doe Defendants") for injunctive relief and damages. LinkedIn alleges as follows:

1. LinkedIn is the world's largest professional network with more than 259 million members in over 200 countries and territories around the globe. LinkedIn's mission is to connect the world's professionals to make them more productive and successful. Through its proprietary platform, LinkedIn allows its members to create, manage and share their professional histories and interests online. In addition, LinkedIn provides valuable services to corporate recruiters and headhunters with its Recruiter product, which allows them to identify among LinkedIn's members top candidates for open positions. At the heart of LinkedIn's platform are its members, who create profiles that serve as their professional online identities and are accessible by any other member.

2. Since May 2013, unknown persons and/or entities employing various automated software programs (often referred to as "bots") have registered thousands of fake LinkedIn member accounts and have extracted and copied data from many member profile pages. This practice, known as data "scraping," is explicitly barred by LinkedIn's User Agreement, which prohibits access to LinkedIn "through scraping, spidering, crawling or other technology or software used to access data without the express written consent of LinkedIn or its Members."

3. The Doe Defendants knowingly and intentionally have breached this and other access and use restrictions in LinkedIn's User Agreement – which they agreed to abide by in registering their accounts – and have circumvented various technical protection barriers employed by LinkedIn. In so doing, they have violated an array of federal and state laws, including the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, et seq. (the "CFAA"), California Penal Code § 502 et seq., and the Digital Millennium Copyright Act, 17 U.S.C. § 1201 et seq. (the "DMCA"), and have engaged in unlawful acts of breach of contract, misappropriation, and trespass.

4. The Doe Defendants' unlawful conduct threatens the LinkedIn platform in several ways. It undermines the integrity and effectiveness of LinkedIn's professional network by polluting it with thousands of fake member profiles. The world's professionals utilize LinkedIn with the expectation that its contents are accurate and its user profiles legitimate. Moreover, by

pilfering data from the LinkedIn site, the Doe Defendants threaten to degrade the value of LinkedIn's Recruiter product, in which LinkedIn has invested substantially over the years. LinkedIn also has suffered additional harms as a result of the Doe Defendants' activities, including, but not limited to, increased strain on and disruption of its network servers and the expenditure of time and resources to investigate and respond to this misconduct.

5. LinkedIn's core guiding value is Members First. Because LinkedIn's members entrust LinkedIn with their professional histories and interests on LinkedIn's site, LinkedIn is committed to earning and keeping its members' trust in everything LinkedIn does, including protecting its members from attempts by third parties to scrape their data.

6. LinkedIn responded swiftly to the Doe Defendants' activities, including promptly disabling the fake member profiles and implementing additional technical protection barriers. In addition to these measures, and to ensure that future incidents do not occur, LinkedIn brings this action to identify the Doe Defendants and to obtain permanent injunctive relief halting their unlawful conduct. The Doe Defendants' activities, if not enjoined, threaten ongoing and irreparable harm to LinkedIn, including to its reputation and substantial consumer goodwill. LinkedIn further is entitled to its actual damages, statutory damages, and/or exemplary damages as a result of the Doe Defendants' misconduct.

JURISDICTION AND VENUE

7. This Court has federal question jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338 because this action alleges violations of federal statutes, including the CFAA, 18 U.S.C. § 1030, et seq., and the DMCA, 17 U.S.C. §§ 1201, et seq. The Court has supplemental jurisdiction over the state law causes of action pleaded herein pursuant to 28 U.S.C. § 1367.

8. Venue is proper in this District under 28 U.S.C. § 1391, because a substantial part of the events or omissions giving rise to the claims occurred in this District.

9. In addition, LinkedIn's User Agreement governing all users' access to and use of the LinkedIn website and LinkedIn's services provides that courts located within the county of Santa Clara, California, shall have jurisdiction over any dispute between LinkedIn and the Doe Defendants.

10. During all relevant times, the Doe Defendants have repeatedly, knowingly, and intentionally accessed LinkedIn's servers located in this judicial district without LinkedIn's authorization, and have contracted for such access, becoming registered LinkedIn members subject to LinkedIn's User Agreement. While accessing LinkedIn's servers, the Doe Defendants made systematic and continuous contacts with this judicial district, and targeted their wrongful acts at LinkedIn, which is headquartered in this judicial district.

11. This is an intellectual property action to be assigned on a district-wide basis under Civil Local Rule 3-2(c).

THE PARTIES

12. LinkedIn is a Delaware corporation with its principal place of business in Mountain View, California.

13. The Doe Defendants are persons and/or entities responsible in whole or in part for the wrongdoing alleged herein. At least for some of the unlawful acts alleged herein, the Doe Defendants registered member accounts on LinkedIn, subject to the LinkedIn User Agreement. LinkedIn is informed and believes that each of the Doe Defendants participated in, ratified, endorsed, or was otherwise involved in the acts complained of and that they have liability for such acts. LinkedIn intends to seek expedited discovery to learn the identity of the Doe Defendants and will amend this Complaint if and when the identities of such persons or entities and/or the scope of their actions becomes known.

FACTS

The LinkedIn Professional Network

14. LinkedIn is the world's largest professional network, with over 259 million members worldwide and over 84 million members in the United States. LinkedIn's mission is to connect the world's professionals to make them more productive and successful.

15. Through its proprietary platform, LinkedIn members are able to create, manage and share their professional identity online, build and engage with their professional network, access shared knowledge and insights, and find business opportunities, enabling them to be more

productive and successful. LinkedIn's broader vision is to create economic opportunity for every member of the global workforce.

16. At the heart of LinkedIn's platform are its members, who create individual profiles that serve as their professional profiles and are accessible by any other member, as well as (unless a member chooses otherwise) anyone with an Internet connection. LinkedIn counts executives from all 2013 Fortune 500 companies as members.

17. LinkedIn's core guiding value is Members First. Because LinkedIn's members entrust LinkedIn with their professional histories and interests on LinkedIn's site, LinkedIn is committed to earning and keeping its members' trust in everything LinkedIn does, including protecting its members from attempts by third parties to scrape their data.

18. The LinkedIn website is an original copyrighted work. Among the significant original elements of the LinkedIn website are the distinctive page layout, design, graphical elements, and organization of member profile pages and the LinkedIn homepage and news feed. LinkedIn's U.S. copyright registrations for the LinkedIn website include Reg. Nos. TX0007355749, TX0007030652, and TX0007455291.

19. LinkedIn has invested and plans to continue to invest substantial time, labor, skill, and financial resources into the development and maintenance of the LinkedIn site.

LinkedIn's User Agreement

20. LinkedIn is available at no cost to anyone who wants to join and who agrees to the terms of LinkedIn's User Agreement and Privacy Policy.[1] A prospective member registers for an account by providing a first name, last name, email address, and password, and agreeing to LinkedIn's User Agreement and Privacy Policy.

21. As described further below, the Doe Defendants registered thousands of fake member accounts as part of their data scraping activities. For each of those accounts, the Doe Defendants agreed to be bound by LinkedIn's User Agreement.

[1] *See* http://www.linkedin.com/legal/user-agreement.

22. LinkedIn's User Agreement explains that members are granted a limited and revocable license to access and use LinkedIn in accordance with the terms of the User Agreement.

23. LinkedIn's User Agreement specifically conditions members' right to access LinkedIn on their agreeing not to do so through the use of data scraping technologies and related conduct. The agreement states, "we grant you a limited, revocable, nonexclusive, nonassignable, nonsublicenseable license and right to access the Services, through a generally available web browser, mobile device or LinkedIn authorized application *(but not through scraping, spidering, crawling or other technology or software used to access data without the express written consent of LinkedIn or its Members)*, to view information and use the Services that we provide on LinkedIn webpages and in accordance with this Agreement." (Emphasis added.)

24. LinkedIn's "Do's and Don'ts" section of its User Agreement reiterates that members may not "undertake … [to] [u]se manual or automated software, devices, scripts robots, other means or processes to access, 'scrape,' 'crawl' or 'spider' any web pages or other services contained in the site." The User Agreement further states that members "will only maintain one LinkedIn account at any given time," "will use [their] real name and only provide accurate information to LinkedIn," and "will not violate any rights of LinkedIn." As described further below, the Doe Defendants' conduct is in flagrant violation of each of these provisions.

LinkedIn's Recruiter Service

25. LinkedIn Recruiter is a premium LinkedIn product that allows corporate recruiters and headhunters to locate and recruit top candidates. Unlike LinkedIn's free, basic accounts for its members, LinkedIn Recruiter requires users to pay a monthly fee for their premium access.

26. LinkedIn Recruiter is one of LinkedIn's fastest growing services. More than 16,000 clients and companies pay to use LinkedIn Recruiter. LinkedIn Recruiter users include human resources departments at some of the most successful companies in the country among thousands of other large, medium and small business and recruiting firms. Ninety of the Fortune 100 companies use LinkedIn Recruiter or another of LinkedIn's premium talent solutions products.

27. Corporate recruiters and headhunters purchase LinkedIn Recruiter memberships in order to search for prospective candidates among LinkedIn's hundreds of millions of member profiles. By using LinkedIn Recruiter's robust and exclusive search tools, recruiters can search the entire LinkedIn network for top candidates' names and profiles. Recruiters may locate and contact members, including passive candidates who may not be looking for a job, by accessing LinkedIn's professional network through LinkedIn Recruiter.

LinkedIn's Technological Safeguards and Security Measures To Protect LinkedIn Against Unauthorized Access

28. LinkedIn fastidiously works to protect the integrity and security of its network and systems. Among other things, it employs an array of technological safeguards and barriers designed to prevent data scrapers and other wrongdoers from gaining unauthorized access to LinkedIn's site.

29. One such safeguard is LinkedIn's FUSE program. FUSE imposes a limit on the activity that an individual LinkedIn user may initiate on the site. This limit is intended to prevent would-be data scrapers utilizing automated technologies from quickly accessing a substantial volume of member profiles.

30. Similarly, LinkedIn's Sentinel program monitors and blocks suspicious activity associated with particular Internet Protocol ("IP") addresses.[2]

31. LinkedIn also anticipated that data scrapers might attempt to create a multitude of fake member accounts. Accordingly, as a secondary layer of protection, LinkedIn implemented its UCV system to thwart this misconduct. The UCV system uses a number of parameters to determine if a new account signup is suspicious. If a suspicious signup is identified, the UCV system imposes barriers intended to separate legitimate prospective members from automated data scraping programs and bots. Specifically, the UCV system introduces a CAPTCHA[3] field that requires prospective members to re-type a word or text that appears in obscured, colored type.

---

[2] An IP address in this context is a numerical label assigned to each access point to the Internet.

[3] CAPTCHA is an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart."

These obscured words or text are legible to a real person – and familiar to those purchasing concert tickets, for instance, as a common step in an online registration process – but difficult for an automated program or bot to recognize. By using CAPTCHAs, the UCV system prevents data scrapers from automatically registering many new and illegitimate member accounts.

32. LinkedIn also employs technical protocols designed to prevent unauthorized automated bots and webcrawlers from accessing otherwise publicly available parts of the LinkedIn site. Known as a robots.txt file, this safeguard provides a set of instructions to any automated technologies visiting the LinkedIn site. While LinkedIn's robots.txt file does permit some webcrawlers (e.g., search engines such as Google or Bing) to view the entire site, it prohibits and is intended to prevent automated programs like those used by data scrapers.

The Doe Defendants' Data Scraping Activities

33. Between May 2013 and the present, the Doe Defendants knowingly and intentionally circumvented FUSE, Sentinel, the UCV system, the robots.txt protocol and/or other LinkedIn security measures in order to engage in their data scraping activities.

34. During this time period, the Doe Defendants created thousands of member accounts (with fake names and contact information) to access and scrape data from many LinkedIn member profiles.

35. In order to create each and every one of these fake member accounts, the Doe Defendants had to agree to abide by the access and use restrictions in LinkedIn's User Agreement, which, *inter alia*, prohibit "scraping, spidering, crawling or other technology or software used to access data without the express written consent of LinkedIn or its Members," and require that members "will only maintain one LinkedIn account at any given time" and "will use [their] real name and only provide accurate information to LinkedIn." The Doe Defendants knowingly violated each of these access and use restrictions in engaging in their unlawful conduct.

36. In May and June 2013, the Doe Defendants circumvented FUSE – which limits the volume of activity for each individual account – by creating thousands of different new member accounts through the use of various automated technologies. Registering so many unique new accounts allowed the Doe Defendants to view hundreds of thousands of member profiles per day.

37. At the same time, the Doe Defendants also circumvented the UCV system by using automated technologies to register thousands of fake member accounts without triggering the UCV system's imposition of CAPTCHAs. The Doe Defendants also circumvented and bypassed LinkedIn's robots.txt file, which specifically bans and is intended to prevent the use of unauthorized automated data scraping programs and bots.

38. In early September 2013, the Doe Defendants again accessed LinkedIn's website and engaged in data scraping through the use of automated data scraping programs. In so doing, the Doe Defendants circumvented LinkedIn's Sentinel program, which limits the number of successive requests made by an IP address or set of IP addresses. They also circumvented the prohibitions set forth in LinkedIn's robots.txt file.

39. LinkedIn initially identified the Doe Defendants' misconduct when it observed that thousands of fake member accounts had collectively viewed many member profiles in a short period of time. LinkedIn determined that the user accounts were fake after close inspection of account details revealed clear patterns of automation. LinkedIn observed that the automated bots that were running these fake accounts would use each account to view a small number of profiles, thereby bypassing and circumventing FUSE's page view restrictions, and then would move on to the next registered account to view additional profiles.

40. LinkedIn conducted an extensive investigation of the Doe Defendants' misconduct. In the course of its investigation, it compiled spreadsheets tracking the IP addresses used by the Doe Defendants. LinkedIn also identified and cataloged the Doe Defendants' fake member profiles, the number of legitimate profiles viewed by each fake member, and the dates and times of the Doe Defendants' activity on the LinkedIn website. LinkedIn disabled the fake member profiles and implemented additional technological safeguards to protect against unauthorized access to the LinkedIn site.

41. As a result of this investigation, LinkedIn determined that the Doe Defendants accessed LinkedIn using a cloud computing platform offered by Amazon Web Services ("AWS"). This platform – called Amazon Elastic Compute Cloud or Amazon EC2 – allows users like the Doe Defendants to rent virtual computers on which to run their own computer programs and

applications. Amazon EC2 provides resizable computing capacity. This feature allows users to quickly scale capacity, both up and down. Amazon EC2 users may temporarily run hundreds or thousands of virtual computing machines. The Doe Defendants used Amazon EC2 to create virtual machines to run automated bots to scrape data from LinkedIn's website.

42. As a result of Doe Defendants' use of Amazon EC2, LinkedIn expects to be able to identify the Doe Defendants by serving third-party discovery on AWS.[4] LinkedIn intends to file motions to expedite these discovery requests.

Doe Defendants Have Caused and Threaten Ongoing and Irreparable Injury to LinkedIn

43. By engaging in the data scraping incidents described above, the Doe Defendants have caused, and if not halted will continue to cause, ongoing and irreparable harm to LinkedIn, in a variety of ways.

44. The thousands of fake member profiles created by the Doe Defendants disrupt and degrade LinkedIn's site and services by reducing the accuracy and integrity of the information the site contains. LinkedIn's members expect the site to contain accurate and legitimate professional profiles – not useless fictions crafted by data scrapers.

45. The presence of fake member profiles also impairs legitimate members' ability to identify valid professional contacts. In particular, because LinkedIn enables its members to view which users have viewed their profiles, legitimate LinkedIn users whose profiles have been viewed by a Doe Defendant using a fake account may be confused or misled when they see that an unknown, fake member has viewed their profiles. Indeed, LinkedIn observed some of its valid members attempting to connect with these fake member profiles after noticing that the fake accounts had viewed their profiles.

46. This type of pollution to the LinkedIn network, if not halted, threatens ongoing and irreparable harm to the integrity of the LinkedIn platform and LinkedIn's reputation. LinkedIn

---

[4] *See* http://portal.aws.amazon.com/gp/aws/html-forms-controller/contactus/AWSAbuse#subpoenas (detailing procedures for serving third-party discovery on Amazon to obtain information relating to "suspected abuse of Amazon Elastic Compute Cloud (Amazon EC2)").

also will suffer ongoing and irreparable harm to the value of its consumer goodwill and trust, which LinkedIn has worked hard for years to earn and maintain, if the Doe Defendants' conduct continues.

47. Further, by pilfering member data from the LinkedIn site, the Doe Defendants misconduct threatens to degrade the value of LinkedIn's Recruiter product, which LinkedIn has invested substantially in over the years. On information and belief, the Doe Defendants, who have invested none of their own time and resources into developing and building the LinkedIn platform, have engaged in their scraping activities in an attempt to establish competing recruiting websites and usurp LinkedIn's Recruiter product.

48. The Doe Defendants' misconduct also has imposed significant strains on LinkedIn's servers, including through the use of automated technologies to view many member profiles. The Doe Defendants' illegitimate profile views impaired LinkedIn's ability to dedicate its servers to supporting the activities of legitimate LinkedIn members.

49. LinkedIn has suffered harm to its computer systems, and has expended significant human, financial, and technological resources, including hundreds of hours of employee time, investigating and responding to the Doe Defendants' unlawful activities, at a cost to LinkedIn of more than $5,000.

FIRST CLAIM FOR RELIEF

Computer Fraud and Abuse Act, 18 U.S.C. §1030 et seq.

50. LinkedIn realleges and incorporates by reference all of the preceding paragraphs.

51. LinkedIn's computers and servers are involved in interstate and foreign commerce and communication, and are protected computers under 18 U.S.C. §1030(e)(2).

52. On information and belief, the Doe Defendants knowingly and intentionally accessed LinkedIn's computers and servers without authorization or in excess of the authorization permitted under LinkedIn's User Agreement and in circumvention of various technical barriers – including FUSE, Sentinel, the UCV system, the robots.txt protocol, and additional safeguards – LinkedIn has employed to protect LinkedIn's computers and servers from unauthorized access.

53. On information and belief, after gaining unauthorized access to LinkedIn's computers and servers, the Doe Defendants obtained and used valuable information from LinkedIn's protected computers and servers in transactions involving interstate or foreign communications in violation of 18 U.S.C. § 1030(a)(2). This information includes, among other things, the contents of many LinkedIn member profiles, and this use, on information and belief, includes, among other things, distributing that content to others.

54. The Doe Defendants knowingly, willfully, and with an intent to defraud, accessed LinkedIn's computers and servers without authorization or in excess of authorization and obtained valuable information from LinkedIn's computers and servers that, on information and belief, the Doe Defendants used to obtain something of value in violation of 18 U.S.C. § 1030(a)(4).

55. LinkedIn has suffered damage and loss by reason of these violations, including, without limitation, harm to LinkedIn's computer systems, expenses associated with being forced to investigate and respond to the unauthorized access and abuse of its computers and servers, and other losses and damage in an amount to be proven at trial, in excess of $5,000 aggregated over a one year period.

56. In addition, LinkedIn has suffered and will continue to suffer irreparable harm, and its remedy at law is not itself adequate to compensate it for injuries inflicted by the Doe Defendants. Accordingly, LinkedIn is entitled to injunctive relief.

SECOND CLAIM FOR RELIEF

California Comprehensive Computer Access and Fraud Act, Cal. Penal Code §502 et seq.

57. LinkedIn realleges and incorporates by reference all of the preceding paragraphs.

58. The Doe Defendants wrongfully obtained and used valuable information from LinkedIn's site, as alleged above.

59. The Doe Defendants knowingly, fraudulently, and without permission accessed or caused to be accessed LinkedIn's computers, computer systems, and/or computer network in violation of Cal. Penal Code § 502(c)(7).

60. The Doe Defendants knowingly, fraudulently, and without permission took, copied and made use of data, and files from LinkedIn's computers, computer systems, and/or computer

networks, including to wrongfully control such data, in violation of Cal. Penal Code § 502(c)(1) &(2).

61. The Doe Defendants knowingly, fraudulently, and without permission disrupted or caused the disruption of LinkedIn's computer services to authorized users of LinkedIn's computers, computer systems, and/or computer networks in violation of Cal. Penal Code § 502(c)(5).

62. As a direct and proximate result of the Doe Defendants' unlawful conduct, the Doe Defendants have caused damage to LinkedIn in an amount to be proven at trial. LinkedIn is also entitled to recover its reasonable attorney's fees pursuant to California Penal Code §502(c).

63. LinkedIn believes that the Doe Defendants' acts were willful and malicious in that Defendants' acts described above were done with the deliberate intent to improve the Doe Defendants' business at LinkedIn's expense. LinkedIn is therefore entitled to punitive damages.

64. In addition, LinkedIn has suffered and will continue to suffer irreparable harm, and its remedy at law is not itself adequate to compensate it for injuries inflicted by the Doe Defendants. Accordingly, LinkedIn is entitled to injunctive relief.

THIRD CLAIM FOR RELIEF

Violations of The Digital Millennium Copyright Act, 17 U.S.C. § 1201 et seq.

65. LinkedIn realleges and incorporates by reference all of the preceding paragraphs.

66. LinkedIn employs various layers of technological protections – including FUSE, Sentinel, the UCV system, the robots.txt protocol, and additional safeguards – to protect LinkedIn's computers and servers from unauthorized access. These technological protection measures effectively control access to the copyrighted materials on LinkedIn's servers, including the LinkedIn website, member profile pages, and the LinkedIn homepage and news feed, and protect LinkedIn's exclusive rights in these copyrighted materials.

67. Despite LinkedIn's best efforts to protect the LinkedIn site from the Doe Defendants' unauthorized access, the Doe Defendants circumvented LinkedIn's technological safeguards – including FUSE, Sentinel, the UCV system, the robots.txt protocol, and additional

safeguards – and gained unauthorized access to LinkedIn's copyrighted materials, including without limitation the copyrighted LinkedIn website, in violation of 17 U.S.C. § 1201(a).

68. As a result of the Doe Defendants' wrongful acts, LinkedIn has suffered, is continuing to suffer, and will continue to suffer damages to be proven at trial. LinkedIn is further entitled to all profits attributable to the Doe Defendants' wrongful acts to be proven at trial. Alternatively, upon its election at any time before final judgment is entered, LinkedIn is entitled to recover statutory damages from the Doe Defendants pursuant to 17 U.S.C. § 1203 for each act of circumvention committed by the Doe Defendants.

69. The Doe Defendants' circumventions also have caused LinkedIn irreparable harm. Unless restrained and enjoined, the Doe Defendants will continue to commit such acts. LinkedIn's remedies at law are not adequate to compensate it for these inflicted and threatened injuries, and thus LinkedIn is entitled to injunctive relief as provided by 17 U.S.C. § 1203.

FOURTH CLAIM FOR RELIEF

Breach of Contract

70. LinkedIn realleges and incorporates by reference all of the preceding paragraphs.

71. Use of the LinkedIn website and use of LinkedIn services are governed by and subject to the User Agreement.

72. LinkedIn members are presented with the User Agreement and must affirmatively accept the User Agreement to register for a LinkedIn account.

73. At all relevant times, LinkedIn also prominently displayed a link to the User Agreement on LinkedIn's homepage.

74. The Doe Defendants accessed the LinkedIn website and affirmatively accepted and agreed to the User Agreement to, among other things, create the fake member profiles that enabled the Doe Defendants to access LinkedIn user profiles and scrape data from LinkedIn's website.

75. The User Agreement is enforceable and binding on the Doe Defendants.

76. The Doe Defendants repeatedly accessed the LinkedIn website with knowledge of the User Agreement and all of its prohibitions. Despite their knowledge of the User Agreement and its prohibitions, the Doe Defendants accessed and continue to access the LinkedIn website to,

among other things, scrape, crawl, or use other automated technology or software to gain access to the LinkedIn website without the consent of LinkedIn. Moreover, the Doe Defendants maintained more than one account (indeed, thousands of accounts) at any given time, and did not provide their real names or provide accurate information to LinkedIn.

77. LinkedIn has been unable to contact the Doe Defendants to demand that they cease and desist their data scraping and other LinkedIn-related activities because LinkedIn does not know the identifies of the Doe Defendants.

78. The Doe Defendants' actions, as described above, have willfully, repeatedly, and systematically breached the User Agreement.

79. LinkedIn has performed all conditions, covenants, and promises required of it in accordance with the User Agreement.

80. The Doe Defendants' conduct has damaged LinkedIn, and caused and continues to cause irreparable and incalculable harm and injury to LinkedIn.

81. LinkedIn is entitled to injunctive relief, compensatory damages, and/or other equitable relief.

FIFTH CLAIM FOR RELIEF

Trespass

82. LinkedIn realleges and incorporates by reference all of the preceding paragraphs.

83. The Doe Defendants intentionally, and without authorization, accessed and interacted with LinkedIn, including without limitation, LinkedIn's website, computer systems and servers.

84. The Doe Defendants' access to LinkedIn and the information contained therein required the Doe Defendants to abide by the User Agreement. By violating the terms of the User Agreement, and LinkedIn's express efforts to combat their activities, the Doe Defendants unlawfully gained access to and interfered and intermeddled with LinkedIn, its website, computer systems, and its servers.

85. The Doe Defendants' unauthorized interference with and access to LinkedIn, its website, computer systems, and its servers, among other harms, reduces LinkedIn's capacity to service its users because it occupies and uses LinkedIn's resources.

86. The Doe Defendants' conduct constitutes trespass that has harmed and will continue to harm LinkedIn. As a result, LinkedIn has been and will continue to be damaged.

87. LinkedIn has suffered and will continue to suffer irreparable harm, and its remedy at law is not itself adequate to compensate it for injuries inflicted by the Doe Defendants. Accordingly, LinkedIn is entitled to injunctive relief.

SIXTH CLAIM FOR RELIEF

Misappropriation

88. LinkedIn realleges and incorporates by reference all of the preceding paragraphs.

89. LinkedIn has invested substantial time, labor, skill, and financial resources into the creation and maintenance of LinkedIn, its computer systems and servers, including system and server capacity, as well as the content on the LinkedIn website, which is time sensitive.

90. Without authorization, the Doe Defendants wrongfully accessed LinkedIn's website, computer systems and servers, and obtained data from the LinkedIn site without having to make the substantial investment in time, labor, skill, and financial resources made by LinkedIn.

91. On information and belief, the Doe Defendants compete with LinkedIn and have made or intend to make data from the LinkedIn site available to their customers and other third parties. As such, the Doe Defendants' use of LinkedIn's computer systems and servers, including system and server capacity, as well as data from the LinkedIn site, constitutes free-riding on LinkedIn's substantial investment of time, effort, and expense.

92. As a result of this misappropriation, the Doe Defendants wrongfully compete, and/or enable others to compete, with LinkedIn, and LinkedIn has been forced to expend additional time and resources, including but not limited to, investigating and responding to the Doe Defendants' activities.

93. LinkedIn has been and will continue to be damaged as the result of the Doe Defendants' acts of misappropriation.

94. LinkedIn has suffered and will continue to suffer irreparable injury, and its remedy at law is not itself adequate to compensate it for injuries inflicted by the Doe Defendants.

PRAYER FOR RELIEF

WHEREFORE, LinkedIn prays that judgment be entered in its favor and against the Doe Defendants, as follows:

1. A preliminary injunction and permanent injunction enjoining and restraining all Doe Defendants, their employees, representatives, agents, and all persons or entities acting in concert with them during the pendency of this action and thereafter perpetually from accessing or using LinkedIn's website for any commercial purpose whatsoever.

2. An order requiring the Doe Defendants to destroy all documents, data, and other items, electronic or otherwise, in their possession, custody, or control, that were wrongfully copied from LinkedIn's website.

3. An award to LinkedIn of restitution and damages, including, but not limited to, compensatory, statutory, treble damages, and punitive damages, as permitted by law;

4. An award to LinkedIn of its costs of suit, including, but not limited to, reasonable attorney's fees, as permitted by law; and

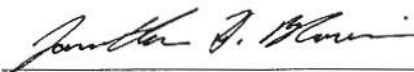
5. Such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

LinkedIn hereby demands a jury trial of all issues in the above-captioned action that are triable to a jury.

DATED: January 6, 2014

MUNGER, TOLLES & OLSON

By: 

JONATHAN H. BLAVIN

Attorneys for LinkedIn Corportation